

HT1711

CLAIMS

1 1. A biometric authentication system comprising:
2 a mobile storage device with a computing function having
3 a tamper-resistance; and
4 a reader/writer having a tamper-resistance for
5 reading/writing information from/into said mobile storage
6 device,
7 wherein said reader/writer includes:
8 a biological information input device for inputting
9 biological information,
10 preprocessing the biological information inputted by
11 said biological information input device, and
12 transmitting intermediate information thus preprocessed
13 to said mobile storage device, and
14 wherein said mobile storage device includes a template
15 of biological information and a secret key to be used for
16 electronic authentication;
17 compares said intermediate information with said
18 template; and
19 makes said secret key available upon a match after
20 comparing.

HT1711

1 2. A biometric authentication system according to Claim 1,
2 wherein,
3 said biological information is fingerprint information,
4 said reader/writer transmits, sequentially to said
5 mobile storage device, a fingerprint image information
6 necessary for a fingerprint identification, and
7 said mobile storage device performs the fingerprint
8 identification by processing said fingerprint image
9 information sequentially.

1 3. A biometric authentication system according to Claim 1,
2 wherein,
3 said biological information is fingerprint information,
4 information for correcting a positional displacement
5 between a registered fingerprint recorded in said template and
6 an input fingerprint that is newly inputted is calculated by
7 using a core position of the fingerprint,
8 a small image in the vicinity of a featuring point of
9 said registered fingerprint is retrieved by performing
10 matching in the vicinity of coordinates of an image of said
11 inputted fingerprint, the positional displacement of the
12 coordinates having been corrected, and
13 said fingerprint image is determined to be identical to
14 said template according to the number of matched small images.

HT1711

1 4. A biometric authentication system according to Claim 3,
2 wherein,
3 a normal vector of a ridge is retrieved, and
4 a position where said normal vector largely changes is
5 determined as a core of the fingerprint.

1 5. A biometric authentication system according to Claim 1,
2 wherein,
3 said biological information is fingerprint information,
4 information for correcting a positional displacement
5 between a registered fingerprint recorded in said template and
6 an input fingerprint that is newly inputted is calculated by
7 forming images having specific luminance distributions in the
8 peripheries of individual featuring points with regard to the
9 input fingerprint and the registered fingerprint, and by
10 correlating said images therebetween,
11 a small image in the vicinity of a featuring point of
12 said registered fingerprint is retrieved by performing
13 matching in the vicinity of coordinates of an image of said
14 inputted fingerprint, the positional displacement of the
15 coordinates having been corrected, and
16 said fingerprint image is determined to be identical to
17 said template according to the number of matched small images.